

Corrected Exhibit

17

to

J. Campbell Miller
Declaration (ECF 105-13)
Exhibit filed at ECF
105-23

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF INDIANA**

CASE NO.: 1:24-cv-00779-JPH-MKK

MAX MINDS, LLC,

Plaintiff,

v.

TRIANGLE EXPERIENCE GROUP, INC.,
ROBERT EDWARD CLARE, JEFFREY
MASE, KEVIN G MULLICAN and JOHN
DOES 1-10,

Defendants.

**PLAINTIFF MAX MINDS, LLC'S AMENDED VERIFIED ANSWERS AND
OBJECTIONS TO DEFENDANT TRIANGLE EXPERIENCE GROUP, INC.'S FIRST
SET OF INTERROGATORIES**

Plaintiff MAX MINDS, LLC, by and through its undersigned counsel, and pursuant to Rule 33 of the Federal Rules of Civil Procedure, hereby serves its Answers and Objections to Defendant's First Set of Interrogatories, as follows:

INTERROGATORIES

1. Identify in detail those portions of the Software's source code You allege constitute trade secrets.

ANSWER:

The entire source code of all relevant versions of MAX's Software is a trade secret of the plaintiff.

2. Identify in detail each instance You allege TEG exposed Max's alleged trade secrets to the public or otherwise endangered Max's alleged trade secrets, as stated, for example, in Counts I and II of Your Complaint and pages 8-9 of Your memorandum of law in support of Your preliminary injunction motion.

SRIPLAW

CALIFORNIA ♦ GEORGIA ♦ FLORIDA ♦ INDIANA ♦ TENNESSEE ♦ NEW YORK ♦ TEXAS

ANSWER:

TEG exposed Max's trade secrets to the public on the following Uniform Resource Locators ("URLs"):

- (1) <https://vjoc-c4map.com/>
- (2) <https://vjoc-c4map.com/admin>
- (3) <https://www.devvjoc-qa.com/>
- (4) www.devvjoc-qa.com/admin
- (5) <https://www.devvjoc.com/>
- (6) <https://www.devvjoc.com/admin>

At each URL listed above, Max's source code for Haptic Federal was exposed to the public.

The source code for Haptic Federal is Max's trade secret. The trade secret source code was exposed from at least March 1, 2024 when Max discovered it to May 20, 2024 when Max confirmed it was removed. The source code may have been exposed for longer since the Google search engine indexing operations indicate www.vjoc-c4map.com was first indexed April 12, 2023; www.devvjoc-qa.com was first indexed December 1, 2023; www.devvjoc.com was indexed either sometime in November 2023 or as late as December 1, 2023.

Max is not aware of other instances or locations where TEG exposed Max's trade secrets to the public at this time. This is a topic of discovery and discovery is continuing

3. Identify in detail the nature of any national security threats that You claim resulted or are resulting from TEG's alleged exposure of the Software's source code and any steps You took or are taking to mitigate such alleged threats.

ANSWER:

According to TEG, Max's Haptic Federal software is currently being used by the Department of Defense on the front lines of the United States Military endeavors, including in the Israel-Hamas conflict and in the war in Ukraine.

TEG's claims that they are using the software on the front lines are supported by the following three articles which mention the DoD's use of VJOC software (the name TEG uses for Max's software).

- https://www.ai.mil/docs/ADOD24/2024_Advantage_DoD_Conference_Apps_for_Decision_Advantage_v3.pdf
- <https://api.army.mil/e2/c/downloads/2024/06/06/fe9e0a11/24-852-1.pdf>
- <https://warroom.armywarcollege.edu/podcasts/gfim/>

Note that whether or not Haptic Federal systems are operational while connected to the public internet does not matter because threats internal to DOD can always exist, and the threat of loss of technological advantage and intelligence gather are still a factor. Thus, the mere fact that Haptic Federal may not be deployed on the public internet does not eliminate the risk posed by TEG's exposure of the Haptic Federal source code on the internet.

The key areas of potential damage in this case concern:

Vulnerability Exploitation

Exposed source code allows adversaries to identify and exploit vulnerabilities:

- Security flaws can be discovered and weaponized by hostile actors
- Attackers can develop targeted exploits for specific DoD systems
- Zero-day vulnerabilities may be uncovered and used in surprise attacks

Operational Compromise

Access to source code can reveal critical operational information:

- Adversaries can gain insights into DoD capabilities and limitations
- Operational plans and strategies may be inferred from code logic
- Sensitive algorithms and decision-making processes could be exposed

Communications and Logistics Disruption

Exposed code can lead to disruptions in vital DoD functions:

- Attackers could degrade or disrupt communications systems in crisis situations
- Logistics and supply chain management could be compromised or manipulated
- Data corruption in critical systems may go undetected, leading to operational failures

Loss of Technological Advantage

Source code exposure can erode the DoD's technological edge:

- Adversaries may replicate or counter advanced capabilities
- Proprietary algorithms and innovations could be stolen
- The first-mover advantage in certain technologies may be lost

Increased Cyber Attack Surface

Exposed source code expands opportunities for cyberattacks:

- Attackers gain a detailed blueprint of the system's architecture
- Security measures and countermeasures become visible to adversaries
- Potential for more sophisticated and targeted cyber operations increases

Intelligence Gathering

Source code can provide valuable intelligence to adversaries:

- Code comments and documentation may reveal sensitive information

- Development patterns could expose organizational structures and priorities
- Embedded data or constants might disclose classified details

Insider Threat Amplification

Source code access can exacerbate insider threat risks:

- Malicious insiders gain deeper knowledge of system vulnerabilities
- Potential for creating backdoors or hidden functionalities increases
- Insiders could more easily exfiltrate or manipulate sensitive data

By compromising the confidentiality and integrity of mission-critical software, the exposure of Max's Haptic Federal source code may have significantly impacted national security.

In addition to the above factors, the exposure of Max's Haptic Federal source code could reveal the internal logic, algorithms, and implementation details of that software. If attackers can understand how the software functions at a deeper level, they might be able to identify and exploit vulnerabilities in the software that have not been detected.

If there are vulnerabilities in the source code, the subsequent discovery of those vulnerabilities due to or after source code exposure could complicate the process of patching and updating the software. There might be increased scrutiny or pressure to address issues quickly, especially if the software is critical to national security.

If the software was exploited by malicious attackers either inside or outside the DOD, such attacks could impact defense operations, critical infrastructure, and data integrity, leading to potentially severe national security implications.

The Department of Justice is aware of the dangers of such exposure and have issued statements on the issue including the following: (1) <https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative> and (2)

<https://www.justice.gov/opa/pr/staffing-company-pay-27m-alleged-failure-provide-adequate-cybersecurity-covid-19-contact>.

4. Identify in detail how the public is being “defrauded and misled” and/or “confused and defrauded” by TEG’s continued servicing of its federal government customers as alleged, inter alia, on page 22 of Your memorandum of law in support of Your preliminary injunction motion.

ANSWER:

TEG removed the “Haptic” source identifier from the login page for the software and changed the source identifier and name to “C4MAP” in some cases and “VJOC” in others.

“C4MAP” and “VJOC” are names TEG uses. TEG was not authorized to change the names of the software. The public that encountered Max’s software was therefore defrauded and misled as to the source and origin of Max’s software.

TEG’s website (<https://www.triangleexperience.com/>) makes no mention of Max’s rights in and to the Haptic Federal software that TEG promotes there. As a result, members of the public who are potential customers are misled and defrauded to believe that Haptic Federal is TEG’s software, not Max’s software.

Online marketplaces that sell products and services to military, civilian and allied governments, such as CHESS IT E-Mart (<https://chess.army.mil>) and SupplyCore (<https://www.supplycore.com/brands/triangle-experience-group/>) continue to promote MAX’s Haptic Federal software as TEG’s own software.

By falsely attributing the software to TEG, members of the public including customers are being defrauded and misled into believing that TEG is the creator and is capable of

supporting (and is the only one who is capable) and servicing the Haptic Federal software, yet this is false.

Discovery is ongoing and Max reserves the right to supplement or amend this interrogatory as more information comes to light.

5. Identify in detail those portions of the Software’s source code You allege are protected elements and those portions You allege are unprotected elements, as necessary to conduct a substantial similarity analysis for Your copyright infringement claims.

ANSWER:

The entire source code for Max’s Haptic Federal software is protected by copyright and trade secret.

The entire source code for Max’s Haptic Federal software meets the definition of a trade secret and no further detail as to “protected elements” is necessary under the DTSA or IUTSA.

The entire source code for Max’s Haptic Federal software is protected by copyright. There are two reasons for this.

First, the entire source code was written originally and creatively by employees or independent contractors of Max and Max owns all the rights to the source code as a work for hire or by assignment.

Second, to the extent that the source code contains or makes use of open source or freely available libraries, Max’s use of those libraries in the source code was original and creative in either (1) the code that Max creatively wrote to implement those libraries, or (2) the selection and arrangement of the code that Max creatively chose and arranged to implement those libraries.

Max does not claim copyright protection in purely functional components of its Haptic Federal source code as those purely functional components would either be (1) uncopyrightable under 17 U.S.C. § 102, or (2) entitled to fair use protection under *Google LLC v. Oracle America, Inc.*, 593 U.S. ___, 141 S.Ct. 1183, 209 L.Ed.2d 311 (2021).

Regarding the question's second premise that identification of portions of the source code are protected in order to "conduct a substantial similarity analysis," the question presents a false predicate because it assumes that Max's allegation is that allegation in the complaint against TEG is that TEG's "software" is substantially similar to Max's Haptic Federal software.

The complaint and motion for preliminary injunction make no such claims. The allegations are that TEG is in possession of Max's Haptic Federal software and that the software in TEG's possession is the same as Max's Haptic Federal software. The expert disclosure by Max's expert Robert Zeidman demonstrates this in detail.

6. Identify in detail the precise information You claim constitutes "copyright management information" under 17 U.S.C. § 1202(c) in support of Count V of the Complaint.

ANSWER:

Max's copyright management information (CMI) consists of the title of Max's software at issue in this case: HAPTIC and the EULA which are the terms and conditions portrayed with the work seen in the below screenshots. The use of Max's CMI in connection with Max's Haptic Federal software is shown below.

ACCESS: LOGGING IN

Enter your TAC SIPR credentials on the sign-in page as shown to the right to access the VJOC application.

FULL TAC SIPR EMAIL
"email@xviicorps.army.smil.mil"

TAC SIPR PASSWORD

EULA Checkbox
(Must be checked.)

7. With respect to the “copyright management information” identified in response to Interrogatory No. 6 above, state in detail and describe where and how such “copyright management information” was conveyed by You or TEG in connection with the work or works You rely upon in Count V of the Complaint.

ANSWER:

Max's CMI was conveyed in both the source code and object code for Max's Haptic Federal software.

In source code, the CMI is contained throughout the code and can be located easily by searching "HAPTIC" and by the inclusion of the "EULA."

In object code, the CMI is displayed to the user as shown in the answer to the previous interrogatory.

8. Identify in detail each instance in which TEG allegedly violated the Certification Agreement, include in Your answer the people who committed the violation, the notice provided to TEG of the alleged violation, and the specific resulting harm from the violation.

ANSWER:

Max is currently aware of the following instances where the Certification Agreement was violated:

1. September 13, 2023. On this date, Haptic Federal source code files for Version 3.1.21.8 were provided to TEG by Max's Jennifer Ryan. TEG received the source code files through David McCutchen. Chain of custody documentation required to be completed and provided to Max was never completed and provided by TEG. TEG never returned Chain of custody documentation for this source code transfer.

2. September 22, 2024. On this date, Jennifer Ryan sent notice to Jeff Mase, David Sinnk, David McCutchen, Michael Bowers, and Chad Coles on September 22, 2024 to return chain of custody documentation for this source code transfer. No documentation was ever received. Jeff Mase of TEG responded demanding that Max send the next build of Haptic

Federal and the source code to run security scans. Mase continued to refuse to return signed Chain of Custody documentation.

3. September 25, 2023. On this date, Jennifer Ryan advised TEG through Jeff Mase and David Sinnk that because of TEG's prior complaints that Max was imposing "unnecessary bureaucracy" by demanding compliance with the Certification Agreement, Max would provide Haptic Federal source code version 21.9 before receiving chain of custody documentation for the prior version 21.8 as an "exception." Jennifer Ryan thereafter provided the Haptic Federal Source Code for Version 3.1.21.9 to TEG.

4. On December 1, 2023, Dustin DuBois (Counsel for Max) emailed Richard Kelley (Counsel for TEG) notifying him that Chain of Custody documents had not been received for the September 13, 2023 source code transfer of Haptic Federal Version 3.1.21.8 and the September 25, 2023 source code transfer for Haptic Federal Version 3.1.21.9.

To date, TEG has not returned chain of custody documentation for the transfers of Haptic Federal Source Code version 3.1.21.8 and 3.1.21.9.

In each case above, notice was given by email, slack, text message, and by phone call. The individuals responsible include Robert Clare, Jeffrey Mase, and Mike Bowers.

The harm from violations is detailed in the answer to question 10 below.

9. If You contend that the Software or the Software's source code is not the result of custom software development that was paid for by TEG, as referenced in the "Intellectual Property" section on page 2 of the Joint Venture Agreement, state in detail the factual basis for that contention.

ANSWER:

Max's Haptic Federal software and source code is **not** the result of custom software development that was paid for by TEG.

Max's Haptic Federal software and source code was independently developed by Max. The entire source code and software are original works of authorship of Max that Max owns. The entire source code was written originally and creatively by employees or independent contractors of Max and Max owns all the rights to the source code as a work for hire or by assignment.

TEG is not an author of any portion of Max's Haptic Federal software or source code. TEG did not affix any copyrightable expression in a medium. To the extent that TEG claims that it made "suggestions" to Max, suggestions do not qualify as copyright protected expression or authorship. In addition, TEG has no exclusive rights under section 106 of the Copyright Act with respect to the source code or software that could be violated.

The Joint Venture Agreement (JVA) does not provide a basis for TEG to claim copyright ownership in the Haptic Federal source code or software. The JVA is not a transfer, assignment, or exclusive license under the Copyright Act. The JVA did not and does not provide for TEG to possess or obtain any ownership interest in any of Max's software. None of the provisions of Chapter 2 of the Copyright Act concerning ownership or transfer of copyright are satisfied by the JVA. The JVA cannot be used to circumvent or satisfy the Copyright Act's strict requirements of an express written instrument signed by the owner of copyright to effect a transfer.

Moreover, contemporaneous agreements like the Source Code License Agreement, signed by the CEO of TEG, Robert Clare, supersede the Intellectual Property section of the JVA and acknowledge that Max is the sole owner of the software.

10. Identify and describe in detail each specific instance of irreparable harm Max claims it has suffered and/or is continuing to suffer, including, but not limited to, any and all of the following: “lost customers, lost market share, lost business,” “harm to Max’s business reputation,” “loss of Max’s right to exclude,” “imminent threat to Max’s relationship with customers,” “imminent threat to Max’s intellectual property,” “imminent threat to the national security of this country,” “harm to Max’s negotiating position,” “damage to Max’s goodwill with licensees,” “threats to Max’s business model,” “loss control of Max’s chief asset,” and “Max’s inability to realize the return on its investment.”

ANSWER:

The irreparable harm Max has suffered and continues to suffer from TEG’s violations of law are as follows:

Loss of Competitive Advantage

Max experienced a theft of proprietary, copyrighted and trade secret source code without documentation required by the Certification Agreement, and in violation of the Source Code agreement. This resulted in an immediate and potentially permanent loss of the company's competitive edge in the federal market. This harm was irreparable because:

- Once the code is exposed to TEG, it cannot be made secret again
- TEG gained access to the code can quickly replicate Max’s technology
- Max lost its first-mover advantage and unique selling proposition

Damage to Market Position

Max’s loss of control over its Haptic Federal source code which has led to:

- Loss of market share as TEG releases similar products
- Erosion of Max’s reputation as an innovator

- Max's reduced ability to attract new customers or retain existing ones

These effects on market position are often difficult to quantify and may persist long after the initial theft, making them potentially irreparable.

Incalculable Economic Losses

Max suffered irreparable economic damages:

- Loss of future revenue streams that are difficult to estimate
- Reduction in the company's valuation, affecting its ability to raise capital
- Diminished licensing opportunities for the technology

Threat to Business Model

As a software company, Max's proprietary code forms the core of its business model.

TEG's theft:

- Undermines the entire foundation of the company's operations as it pertains to the federal contracting space especially within DOD
- Potentially renders ongoing research and development efforts for software designed for DOD customers obsolete
- May force Max to make a fundamental shift in the company's strategic direction with respect to the federal and DOD market

Security and Trust Issues

TEG's theft of Max's source code could potentially lead to:

- Increased vulnerability to cyberattacks as detailed above in answer to question one.
- Loss of customer trust and confidence in the company's ability to protect sensitive information

Max continues to be irreparably harmed by TEG's violations of law. TEG's continued possession of Max's Haptic Federal source code violates requirements in agreements that TEG destroy the code and maintain the confidentiality of the code.

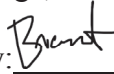

Max has lost control of its source code. Loss of control easily leads to the other types of irreparable harm detailed above.

See also Max's answer to number 3 above.

VERIFICATION

I, Brandon Fischer, hereby swear under the penalty of perjury that I am the Plaintiff in this action, and that I have read the foregoing Answers to Interrogatories and know the contents thereof, and the same are true to the best of my knowledge, information and belief.

Dated: 09/18/2024 _____

By:  _____
Name:  Verified by signNow
09/18/2024 21:18:38 UTC
7174650c9d8c4e92b195
Title: _____

Dated: September 18, 2024

Respectfully submitted,

/s/ J. Campbell Miller

J. CAMPBELL MILLER

Bar Number: 38279-49

campbell.miller@sriplaw.com

SRIPLAW, P. A.

231 South Rangeline Road

Suite H

Carmel, IN 46032

332.600.5599 – Telephone

561.404.4353 – Facsimile

and

JOSEPH A. DUNNE (Pro Hac Vice)

joseph.dunne@sriplaw.com

SRIPLAW, P. A.

175 Pearl Street

Third Floor

Brooklyn, IN 11201

929.200.8446 – Telephone

561.404.4353 – Facsimile

and

JOEL B. ROTHMAN (Pro Hac Vice)

joel.rothman@sriplaw.com

SRIPLAW, P. A.

21301 Powerline Road

Suite 100

Boca Raton, IN 33433

561.404.4335 – Telephone

561.404.4353 – Facsimile

and

PHILIP D SEVER

Bar Number: 25384-49

phil@landownerattorneys.com

SEVER, STORY, WALKER

742 South Rangeline Road
Carmel, IN 46032
317.961.1202 - Telephone

Counsel for Plaintiff Max Minds, LLC

CERTIFICATE OF SERVICE

The undersigned does hereby certify that on September 18, 2024, a true and correct copy of the foregoing document was served by electronic mail to all parties listed below on the Service List.

/s/ J. Campbell Miller

J. CAMPBELL MILLER

SERVICE LIST

Alexandra Wilson Pantos
Krieg Devault LLP
One Indiana Square
Suite 2800
Indianapolis, IN 46204
awilson@kdlegal.com

Marc T. Quigley
Krieg Devault LLP
12800 North Meridian Street
Suite 300
Carmel, IN 46032
mquigley@kdlegal.com

Raighne Coleman Delaney
Stephen Daniel Caruso
Richard Daniel Kelley
Bean, Kinney & Korman, PC
2311 Wilson Boulevard
Suite 500
Arlington, VA 22201
rdelaney@beankinney.com
scaruso@beankinney.com
rkelley@beankinney.com

*Counsel for Triangle Experience Group, Inc.,
Robert Edward Clare, Jeffrey Mase, and
Kevin G Mullican*